

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-51575

(43) 公開日 平成9年(1997)2月18日

(51) Int.Cl.<sup>6</sup>

H 0 4 Q 7/38

識別記号

庁内整理番号

F I

H 0 4 B 7/26

技術表示箇所

1 0 9 R

審査請求 未請求 請求項の数12 O L (全 11 頁)

(21) 出願番号 特願平7-199805

(22) 出願日 平成7年(1995)8月4日

(71) 出願人 392026693

エヌ・ティ・ティ移動通信網株式会社  
東京都港区虎ノ門二丁目10番1号

(72) 発明者 石田 創

東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

(72) 発明者 大貫 雅史

東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

(72) 発明者 中村 寛

東京都港区虎ノ門二丁目10番1号 エヌ・  
ティ・ティ移動通信網株式会社内

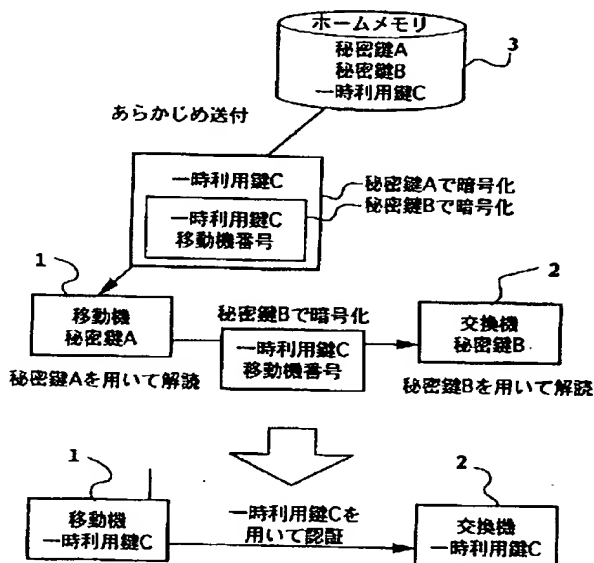
(74) 代理人 弁理士 谷 義一 (外1名)

(54) 【発明の名称】 移動通信における認証方法および移動通信システム

(57) 【要約】

【課題】 認証によるホームメモリアクセス回数を減らす。

【解決手段】 ホームメモリ3が生成した一時利用鍵Cと暗号化された一時利用鍵Cとを移動機1が取得した後、移動機1から暗号化された一時利用鍵Cを交換機2に送信し、交換機2が復号化鍵を用いて暗号化された一時利用鍵Cを復号した後、移動機1と交換機2との間で共有した一時利用鍵Cにより認証を行う。



**【特許請求の範囲】**

【請求項1】 ホームメモリが生成した一時利用鍵と暗号化された一時利用鍵とを移動機が取得した後、前記移動機から前記暗号化された一時利用鍵を交換機に送信し、前記交換機が復号化鍵を用いて前記暗号化された一時利用鍵を復号した後、前記移動機と前記交換機との間で共有した前記一時利用鍵により認証を行うことを特徴とする移動通信における認証方法。

【請求項2】 請求項1において、前記移動機は、あらかじめ定められた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得することを特徴とする移動通信における認証方法。

【請求項3】 請求項1において、前記交換機は、前記復号化鍵を時間の経過に従って変更することによって前記一時利用鍵の利用できる時間を制限することを特徴とする移動通信における認証方法。

【請求項4】 移動機に与えるための一時利用鍵および暗号化された一時利用鍵を生成する手段を具えたことを特徴とするホームメモリ。

【請求項5】 ホームメモリが生成した一時利用鍵および暗号化された一時利用鍵を取得する手段と、前記取得した暗号化された一時利用鍵を交換機に送出する手段と、前記取得した一時利用鍵により前記交換機との間で認証を行う手段とを具えたことを特徴とする移動機。

【請求項6】 移動機から送信された暗号化された一時利用鍵を受信する手段と、前記受信された一時利用鍵を復号化鍵を用いて復号する手段と、前記復号された一時利用鍵により前記移動機との間で認証を行う手段とを具えたことを特徴とする交換機。

【請求項7】 請求項4のホームメモリと、請求項5の移動機と、請求項6の交換機とを具えたことを特徴とする移動通信システム。

【請求項8】 請求項4において、さらに、あらかじめ定められた限定された地域範囲毎に一時利用鍵および暗号化された一時利用鍵を新たに生成する手段を有することを特徴とするホームメモリ。

【請求項9】 請求項5において、さらに、あらかじめ定められた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得する手段を有することを特徴とする移動機。

【請求項10】 請求項6の交換機と、請求項8のホームメモリと、請求項9の移動機とを具えたことを特徴とする移動通信システム。

【請求項11】 請求項6において、前記復号手段は、前記復号化鍵を時間の経過に従って変更する手段を有することを特徴とする交換機。

【請求項12】 請求項4のホームメモリと、請求項5の移動機と、請求項11の交換機とを具えたことを特徴とする移動通信システム。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明はホームメモリのアクセスを減らす認証方式を利用する移動通信における認証方法および移動通信システムにかかわる。

**【0002】**

【従来の技術】図8にRCR STD 27Cに記されている従来の移動通信における認証方法を示す。このシステムは移動機101、交換機102、ホームメモリ103からなる。移動機101とホームメモリ103は秘密鍵Sを共有する。交換機102は移動機101の正当性をチェックする必要がある場合、ホームメモリ103から秘密鍵Sを読み出し、乱数を生成し、移動機101へ乱数を送信する。移動機101は乱数を受信すると秘密鍵Sと乱数を使い認証演算し、結果を交換機102へ送信する。交換機102は乱数と秘密鍵Sを使用して認証演算し、移動機101から受信した認証演算結果と比較する。交換機102は比較結果が一致するとその移動機101は正当であるとみなし、一致しないとその移動機は正当でない移動機とみなす。

【0003】不正移動機は交換機102から乱数を受信しても秘密鍵Sがないため、正しい認証演算ができず、正しい演算結果を返すことができない。その結果交換機102はその移動機が正当でないことがわかる。

**【0004】**

【発明が解決しようとする課題】従来の方式では認証が必要になる度に交換機102はホームメモリ103へアクセスを行った。その結果、認証が頻繁に必要になるとホームメモリアクセスが増え、ホームメモリ103に大きな処理能力が必要となった。

【0005】そこで本発明の目的は以上のような問題を解消した移動通信における認証方法および移動通信システムを提供することにある。

**【0006】**

【課題を解決するための手段】図1は上記課題を解決するための手段を示す。基本的な考え方は、あらかじめ移動機に認証鍵を送っておき、認証が必要になると移動機から交換機に認証鍵を渡すことで、ホームメモリアクセスを減らす方法である。

【0007】移動機1とホームメモリ3は秘密鍵Aを共有する。また、交換機2とホームメモリ3は秘密鍵Bを共有する。

【0008】ホームメモリ3は、移動機1に固有な一時利用鍵Cを生成する。そして一時利用鍵Cと移動機番号をまとめて秘密鍵Bで暗号化する。さらに一時利用鍵Cとこの秘密鍵Bで暗号化したデータとをまとめ、秘密鍵Aで暗号化する。ホームメモリ3はこの秘密鍵Aで暗号化されたデータを移動機1に送出する。移動機1は秘密鍵Aで暗号化されたデータを受け取ると、このデータを秘密鍵Aを用いて復号化し、一時利用鍵Cと秘密鍵Bで

暗号化されたデータを得て、これを記憶する。

【0009】秘密鍵Aと秘密鍵Bを共に知っているのはホームメモリ3だけであり、この秘密鍵Aで暗号化されたデータはホームメモリ3にしか作れないため、暗号化データの作成に関してはセキュリティが保てる。

【0010】また、他の移動機などは秘密鍵Aを知らないため、暗号化データを盗聴しても、秘密鍵Aで暗号化されたデータの解読はできない。

【0011】次に認証が必要になると、移動機1は交換機2に秘密鍵Bで暗号化されたデータを送信する。交換機2は秘密鍵Bで暗号化されたデータを秘密鍵Bを用いて復号化し、移動機番号と一時利用鍵Cを得る。さらに、移動機番号を確認した後、一時利用鍵Cを用いて移動機1の認証を行う。

【0012】秘密鍵Bを知っているのはホームメモリ3と交換機2のみであるため、移動機1がこの秘密鍵Bで暗号化されたデータを偽造することはできない。また、秘密鍵Bで暗号化されたデータには移動機番号が含まれるため、該当移動機以外がこのデータを利用することもできない。

【0013】また、他人が盗聴しても秘密鍵Bを知らないため、復号化することはできない。

【0014】上記手順により移動機1と交換機2は他人に知られることなく一時利用鍵Cを共有化することができ、この一時利用鍵Cにより交換機2は移動機1の認証ができる。

【0015】暗号解読において、暗号文が多数手にはいるほど、また、平文と暗号文の組み合わせが多数手にはいるほど、暗号が破られ、秘密鍵の秘密性が保てなくなる可能性は高くなる。

【0016】上記において秘密鍵Bは複数の交換機で共通の鍵を使用し、またすべての移動機に対して共通の鍵を使用する。その結果秘密鍵Bの使用頻度は多くなり、秘密鍵Bの秘密が保てない可能性も高くなる。この可能性を減らすため、秘密鍵Bの使用回数を減らす、以下の2つの方法がある。

【0017】図2に第1の方法を示す。移動通信のエリアは着信の呼出エリアを限定するため複数の位置登録エリア(図2では地域1、地域2)に区切られており、移動機1は位置登録エリアを移動する度にホームメモリ3の位置登録エリアを登録する。

【0018】この位置登録エリア毎に秘密鍵Bを変えることで、一つの秘密鍵Bの使用頻度と範囲は限定される。移動機1は位置登録エリアを移行する毎に位置登録と、さらに一時利用鍵Cの受け取りを行う。

【0019】図3に第2の方法を示す。ホームメモリ3は秘密鍵Bを時間と共に変更し、交換機2に配送する。交換機2は発行時間別の秘密鍵Bのリストを持ち、発行時刻により、復号化に使用する秘密鍵Bを使い分ける。一時利用鍵Cには利用期限を設け、利用期限が来ると一

時利用鍵Cと秘密鍵Bを破棄する。

【0020】以上から、請求項1にかかる発明は、ホームメモリが生成した一時利用鍵と暗号化された一時利用鍵とを移動機が取得した後、前記移動機から前記暗号化された一時利用鍵を交換機に送信し、前記交換機が復号化鍵を用いて前記暗号化された一時利用鍵を復号した後、前記移動機と前記交換機との間で共有した前記一時利用鍵により認証を行うことを特徴とする。

【0021】また、請求項2にかかる発明は、請求項1において、前記移動機は、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得することを特徴とする。

【0022】さらに、請求項3にかかる発明は、請求項1において、前記交換機は、前記復号化鍵を時間の経過に従って変更することによって前記一時利用鍵の利用できる時間を制限することを特徴とする。

【0023】さらに、請求項4にかかる発明は、移動機に与えるための一時利用鍵および暗号化された一時利用鍵を生成する手段を具えたことを特徴とする。

【0024】さらに、請求項5にかかる発明は、ホームメモリが生成した一時利用鍵および暗号化された一時利用鍵を取得する手段と、前記取得した暗号化された一時利用鍵を交換機に送出する手段と、前記取得した一時利用鍵により前記交換機との間で認証を行う手段とを具えたことを特徴とする。

【0025】さらに、請求項6にかかる発明は、移動機から送信された暗号化された一時利用鍵を受信する手段と、前記受信された一時利用鍵を復号化鍵を用いて復号する手段と、前記復号された一時利用鍵により前記移動機との間で認証を行う手段とを具えたことを特徴とする。

【0026】さらに、請求項7にかかる発明は、請求項4のホームメモリと、請求項5の移動機と、請求項6の交換機とを具えたことを特徴とする。

【0027】さらに、請求項8にかかる発明は、請求項4において、さらに、あらかじめ定めた限定された地域範囲毎に一時利用鍵および暗号化された一時利用鍵を新たに生成する手段を有することを特徴とする。

【0028】さらに、請求項9にかかる発明は、請求項5において、さらに、あらかじめ定めた限定された地域範囲毎に前記ホームメモリが新たに生成した一時利用鍵および暗号化された一時利用鍵を取得する手段を有することを特徴とする。

【0029】さらに、請求項10にかかる発明は、請求項6の交換機と、請求項8のホームメモリと、請求項9の移動機とを具えたことを特徴とする。

【0030】さらに、請求項11にかかる発明は、請求項6において、前記復号手段は、前記復号化鍵を時間の経過に従って変更する手段を有することを特徴とする。

【0031】さらに、請求項12にかかる発明は、請求項4のホームメモリと、請求項5の移動機と、請求項11の交換機とを具えたことを特徴とする。

【0032】

【発明の実施の形態】図4に本発明の実施形態の一例を示す。この例は、移動機1と交換機2とホームメモリ3とからなる。

【0033】移動機1は、秘密鍵Aを記憶する秘密鍵A記憶部4、一時利用鍵Cを記憶する一時利用鍵C記憶部5、暗号化データを記憶する暗号化データ記憶部6、復号化機能部7、入出力（送受信）部8および制御部9を有する。制御部9はこれらの各構成4～8を制御し、後述（図6、図7）の各制御手順に従う制御を行うものであって、そのためのCPU、ROM、RAM等から構成される。入出力部8は各記憶部4～6および制御部9と交換機2およびホームメモリ3との間のデータ（信号）の授受を行う。復号化機能部7は各記憶部4～6内のデータを参照して入力されたデータを必要に応じて復号する。

【0034】交換機2は、時間別秘密鍵Bリスト記憶部10、復号化機能部11、入出力部12および制御部13を有する。制御部13はこれらの各構成10～12を制御し、後述（図5～図7）の各制御手順に従う制御を行うものであって、そのためのCPUおよびROM、RAM、ハードディスク等の記憶手段等から構成される。入出力部12は、記憶部10および制御部13と移動機1およびホームメモリ3との間のデータ（信号）の授受を行う。時間別秘密鍵Bリスト記憶部10は、発行時刻とこれに対応する秘密鍵Bのリストを記憶する。復号化機能部11は記憶部10内のデータを参照して入力されたデータを必要に応じて復号する。

【0035】ホームメモリ3は、移動機毎の秘密鍵Aを記憶する秘密鍵A記憶部14、地域別秘密鍵Bリスト記憶部15、暗号化機能部16、入出力部17および制御部18を有する。制御部18はこれらの各構成14～17を制御し、後述（図5、図6）の各制御手順に従う制御を行うものであって、そのためのCPUおよびROM、RAM、ハードディスク等の記憶手段等から構成される。入出力部17は各記憶部14、15および制御部18と移動機1および交換機2との間のデータ（信号）の授受を行う。地域別秘密鍵Bリスト記憶部15は、地域とこれに対応する秘密鍵Bのリストを記憶する。暗号化機能部16は、後述のように、各記憶部14、15内のデータ（秘密鍵A、B）によって、一時利用鍵C、移動機番号等を暗号化する。

【0036】図5にホームメモリ3が秘密鍵Bを生成し、交換機2に配送する手順を示す。ホームメモリ3は秘密鍵Bを生成すると、秘密鍵Bを記憶し、秘密鍵Bと使用開始時刻を含む秘密鍵B配送信号により交換機2に秘密鍵Bを配送する。秘密鍵B配送信号を受けた交換機

2は、時間別秘密鍵Bリスト記憶部10に使用開始時刻と秘密鍵Bを記憶する。また、一時利用鍵Cに使用期限がある場合、対応する一時利用鍵Cが期限切れとなり、使用することのない秘密鍵Bを削除しても良い。

【0037】なお、ホームメモリ3において、秘密鍵Bを生成するタイミングは一定時間毎でもよいし、一時利用鍵Cを一定回数発行する毎でもよいし、あるいは不定期間隔でも良い。また、秘密鍵B配送信号が盗聴されると、秘密鍵Bの秘密性が保てなくなるため、十分セキュリティの高い方法で配送する必要がある。

【0038】図6に移動機1が、位置登録エリアの移動や、一時利用鍵Cの期限切れで、ホームメモリ3が新たに一時利用鍵Cを発行する手順を示す。

【0039】移動機1は移動機番号を含む位置登録要求を交換機2に送信する。

【0040】位置登録要求を受信した交換機2は移動機番号からこの移動機1のホームメモリ3を探し、移動機番号を含む認証情報読出要求をそのホームメモリ3に送信する。

【0041】認証情報読出要求信号を受信したホームメモリ3は、該当移動機1のデータを検索し、秘密鍵Sを含む認証情報読出応答を交換機2に送信する。

【0042】認証情報読出応答を受信した交換機2は乱数を生成し、認証要求信号により乱数を移動機1に送信する。

【0043】認証要求信号を要求した移動機1は乱数とあらかじめ持っている秘密鍵Sから認証演算を行い、認証演算結果を含む認証応答信号を交換機2に送信する。

【0044】交換機2は乱数と秘密鍵Sから認証演算を行い、移動機1から受信した認証演算結果と比較する。比較結果が一致しないと、移動機1に位置登録拒否を送信する。比較結果が一致すると、ホームメモリ3に対して移動機番号を含む一時利用鍵発行要求を送信する。

【0045】一時利用鍵発行要求を受信したホームメモリ3は当該交換機にかかる位置登録エリアに登録し、一時利用鍵Cを生成し、秘密鍵Bおよび秘密鍵Aを使用して暗号化データ、すなわち、一時利用鍵Cおよび移動機番号を秘密鍵Bで暗号化し、これと、一時利用鍵Cおよび鍵発行時刻とを秘密鍵Aで暗号化した暗号化データを作り、一時利用鍵発行応答で交換機2に送出する。

【0046】一時利用鍵発行応答を受信した交換機2は、暗号化データを含む位置登録応答を移動機1に送出する。この位置登録応答を受信した移動機1はこれを秘密鍵Aで復号する（この結果、一時利用鍵Cおよび鍵発行時刻が復号され、これらは記憶される）。

【0047】なお、この例においては信号数の削減のため、位置登録と一時利用鍵Cの発行手順を同時に行っているが、分けて行ってもかまわない。また、秘密鍵Sを交換機2に送信して、交換機2が乱数の生成と認証演算を行っていたが、ホームメモリ3で乱数の生成と、認証

演算を行い、交換機には、認証情報読出応答で乱数と認証演算結果を送信してもよい。

【0048】図7に一時利用鍵Cを利用するサービス手順を示す。

【0049】移動機1は、移動機番号、鍵発行時刻、暗号化データを含むサービス要求を交換機2に送信する。この復号化データは、位置登録時に得た暗号化データを、秘密鍵Aで解読することによって得られた秘密鍵Bで暗号化されている暗号化データであり、一時利用鍵Cと移動機番号のデータを含んでいる。

【0050】サービス要求を受信した交換機2は、鍵発行時刻に対応する秘密鍵Bを、時間別秘密鍵Bリスト記憶部10から選び、これによって暗号化データを復号化する。この復号化に失敗すると、交換機2は移動機1にサービス拒否を通知する。また、復号化したデータの中に含まれる移動機番号の値とサービス要求信号中の移動機番号が異なる場合も交換機2は移動機1にサービス拒否を通知する。

【0051】交換機2は、正常に復号化でき、内容が正常であることを確認すると、次に移動機1が一時利用鍵を持っているかどうか確認するために、乱数を生成し、移動機1に乱数を含むローカル認証要求を送信する。

【0052】ローカル認証要求信号を受信した移動機1は乱数と一時利用鍵Cから認証演算を行い、認証演算結果を含む認証応答信号を交換機2に送信する。

【0053】交換機2は乱数と一時利用鍵Cから認証演算を行い、移動機から受信した認証演算結果と比較する。比較結果が一致しないと、移動機1にサービス拒否を送信する。比較結果が一致すると、交換機2はサービスを開始する。

【0054】上記において、鍵発行時刻は時間別秘密鍵Bリスト記憶部10のどの値を利用するかを決めるものであるため、現実の時刻でなく、秘密鍵Bを作りなおす度に増えるような数あるいは、時間別秘密鍵Bリスト記憶部10の中のどの鍵を使用しているか示すようなインデックスでもよい。

【0055】

【発明の効果】本発明によれば、ホームメモリにアクセスすることなく交換機が移動機の正当性を知ることができ、ホームメモリアクセスの回数を減少することができる。

【図面の簡単な説明】

【図1】本発明における課題を解決するための手段を示す図である。

【図2】秘密鍵Bの使用回数を減らすための一方法を説明する図である。

【図3】秘密鍵Bの使用回数を減らすための他の一方法を説明する図である。

【図4】本発明の実施形態の一例を示す図である。

【図5】本発明における制御手順の一例を示す図である。

【図6】本発明における制御手順の他の一例を示す図である。

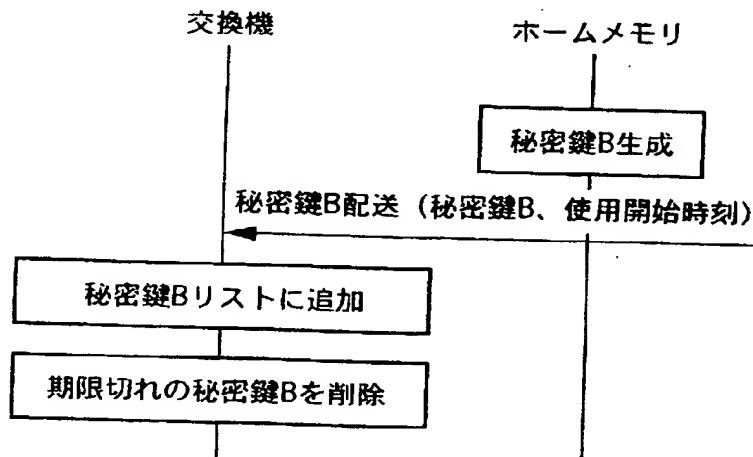
【図7】本発明における制御手順のさらに他の一例を示す図である。

【図8】従来例を示す図である。

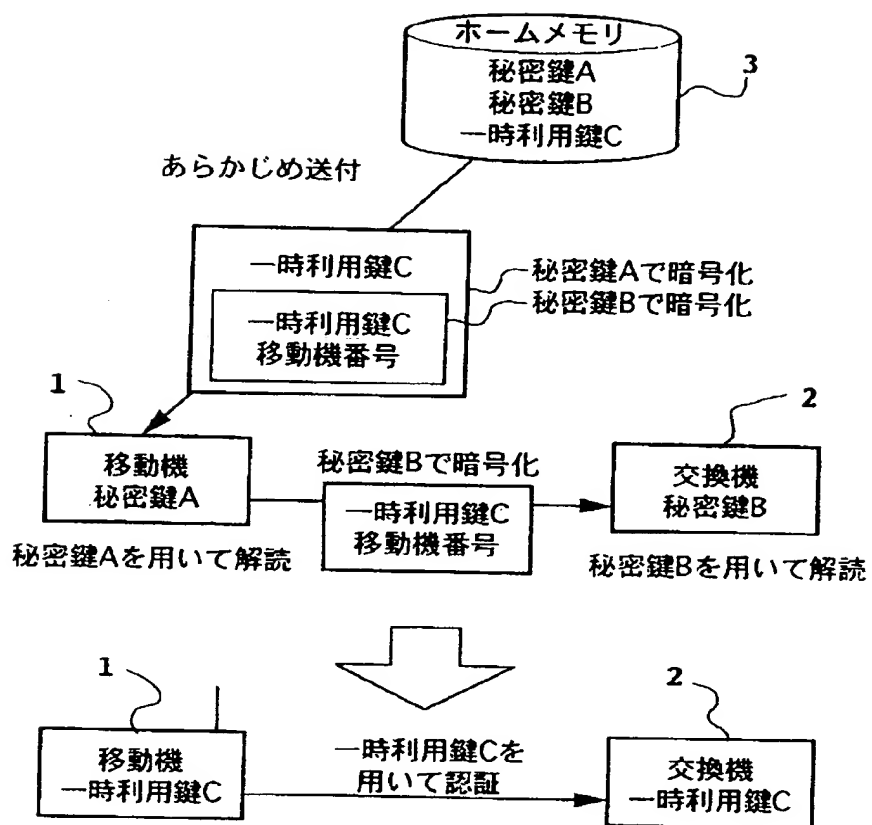
【符号の説明】

- 1 移動機
- 2 交換機
- 3 ホームメモリ

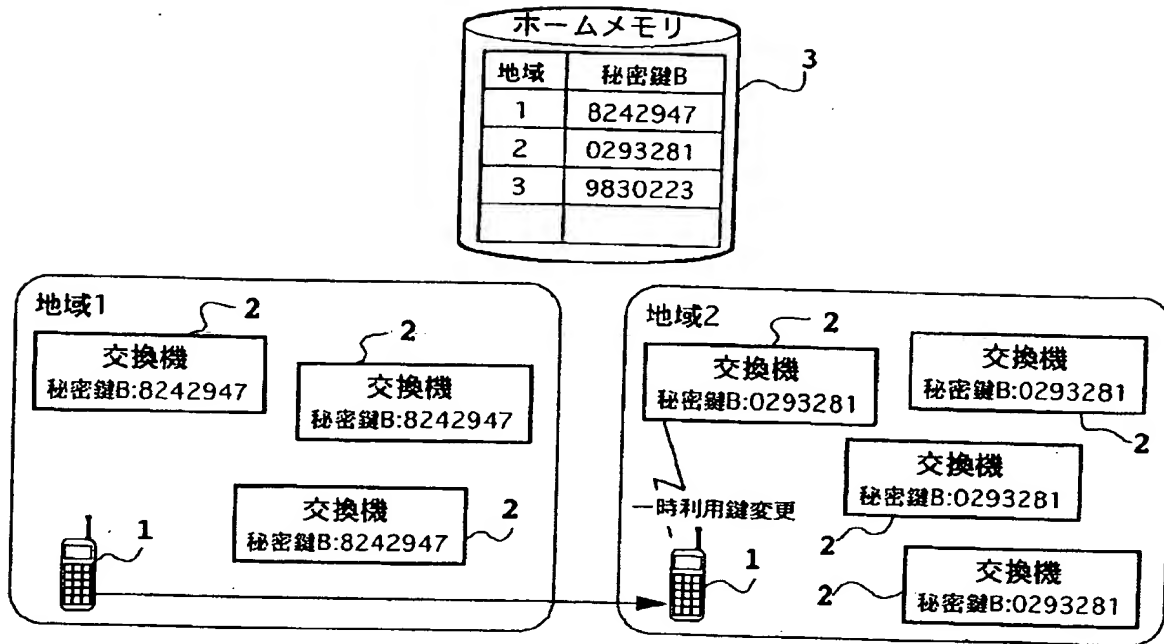
【図5】



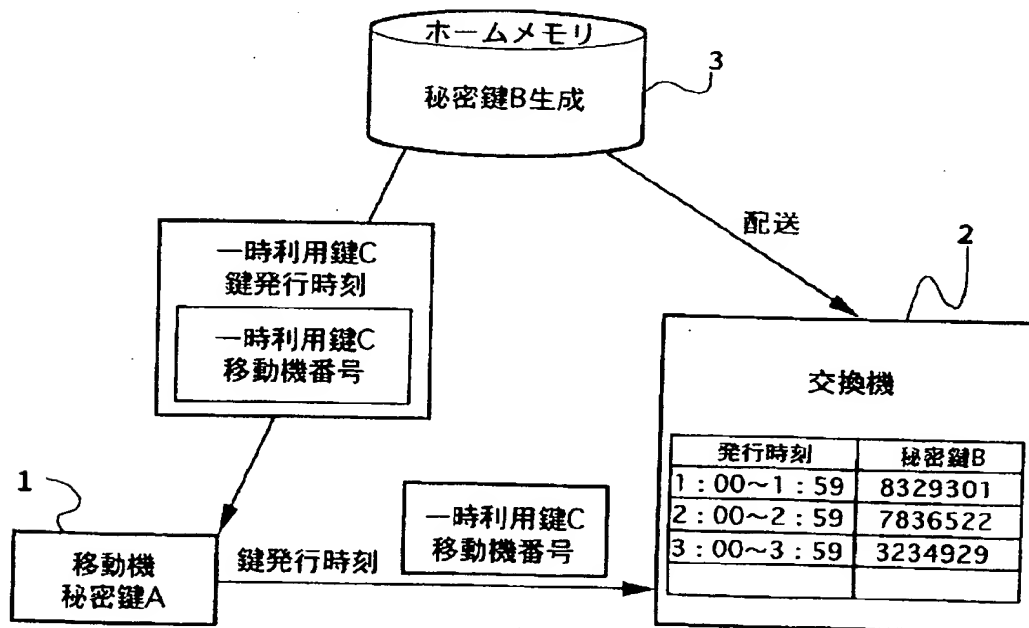
【図1】



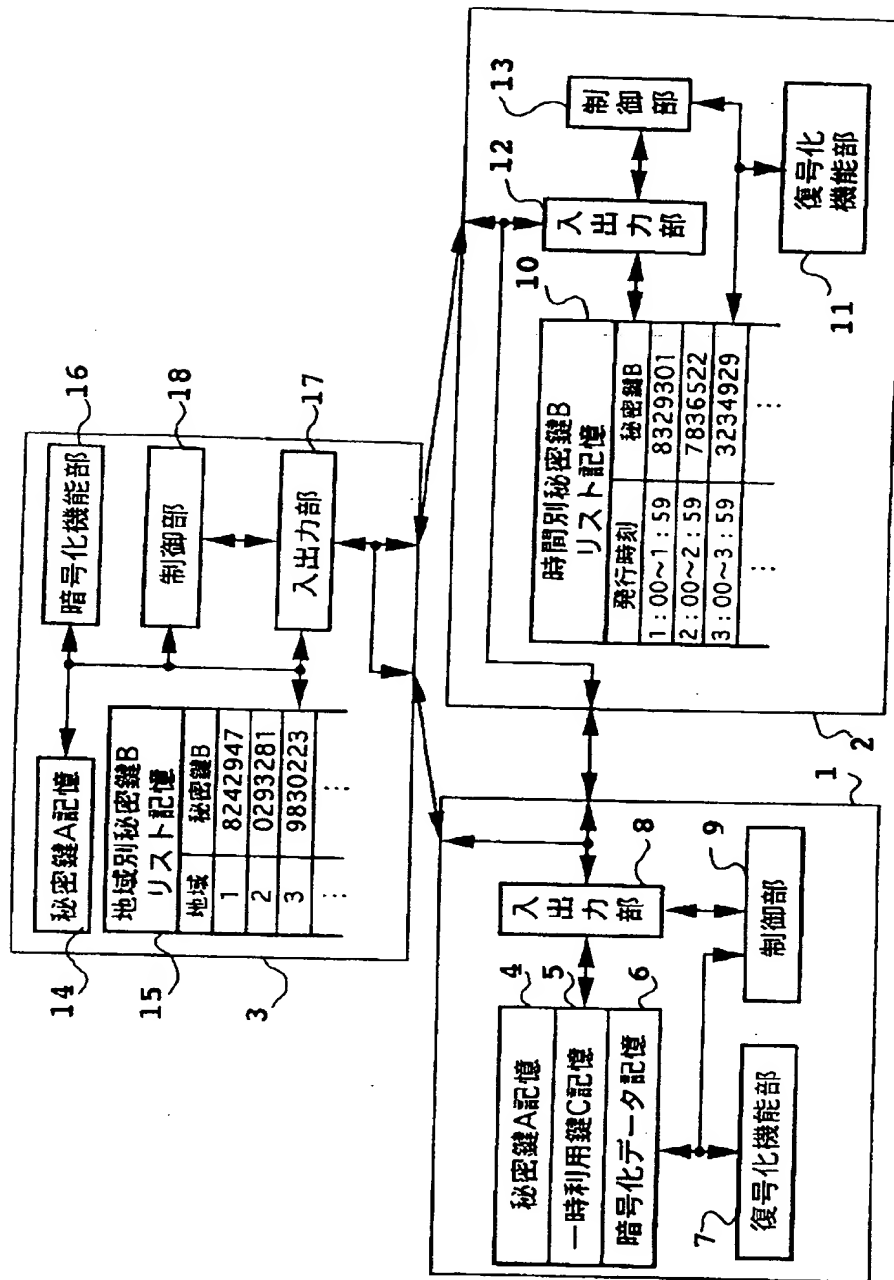
【図2】



【図3】

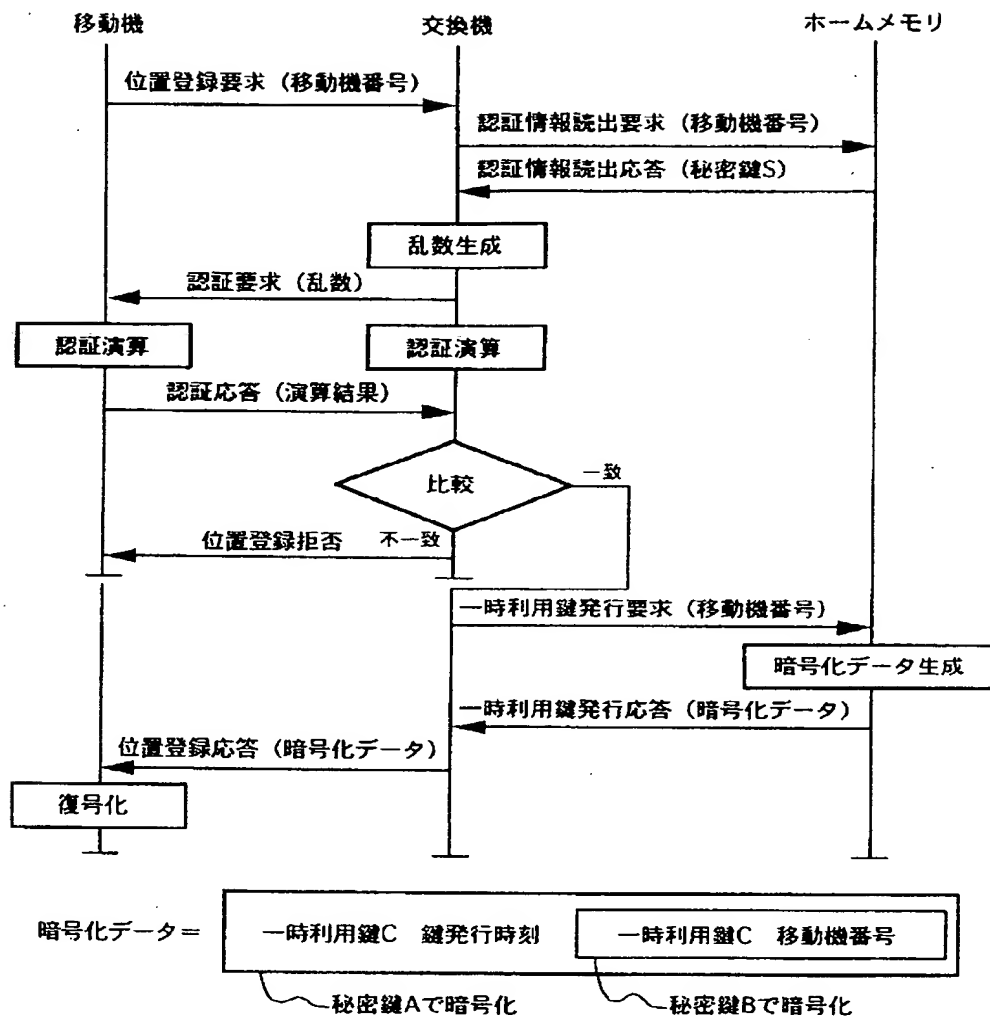


【図4】

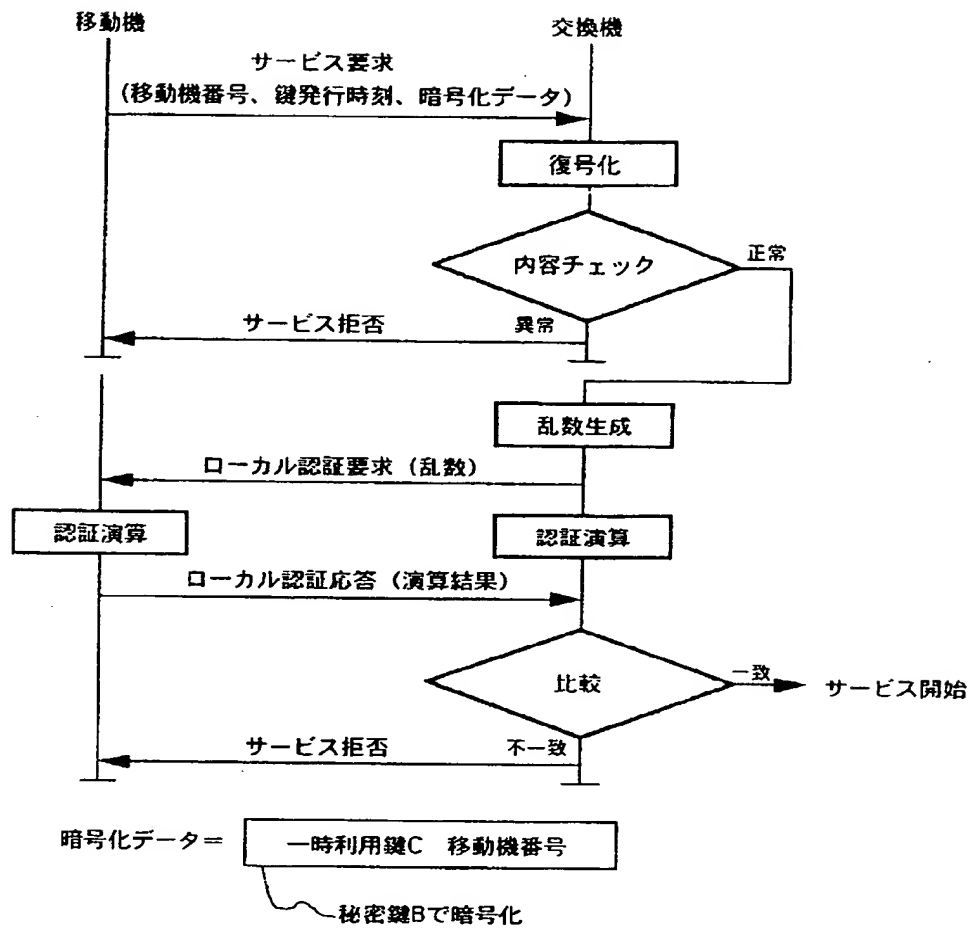




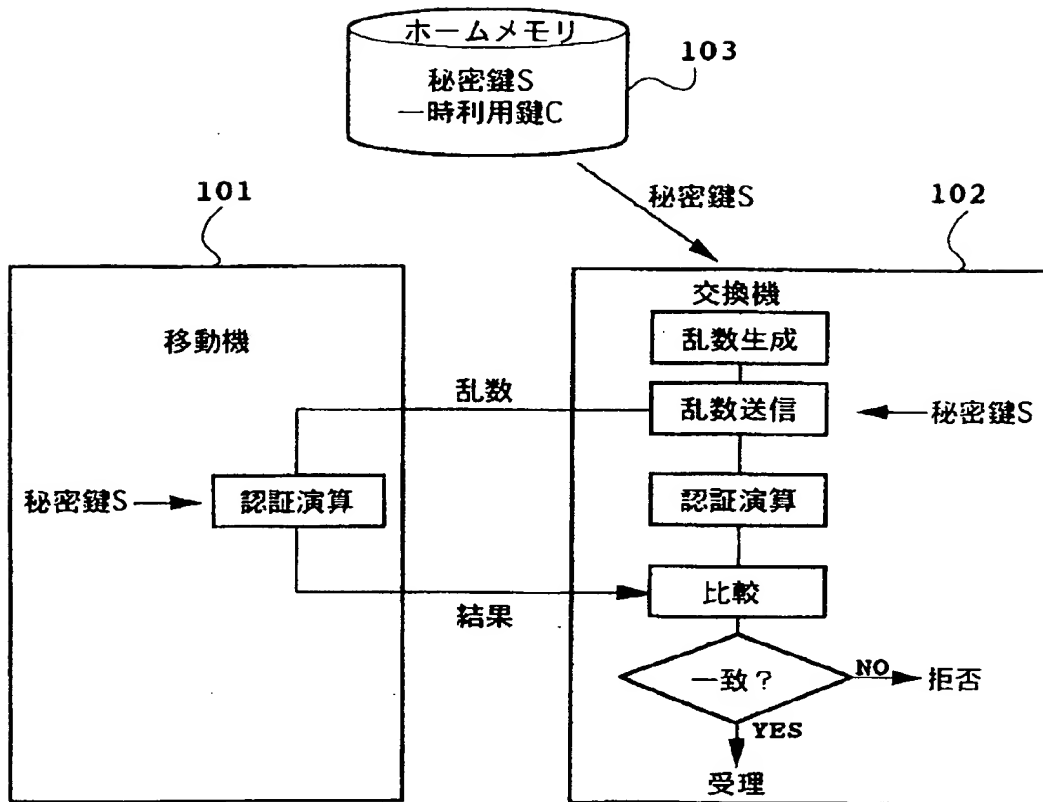
【図6】



【図7】



【図8】



## ABSTRACTS OF JP 09 - 051575

### AUTHENTICATING METHOD FOR MOBILE COMMUNICATION AND MOBILE COMMUNICATION SYSTEM

#### Abstract:

**PROBLEM TO BE SOLVED:** To reduce home memory access by sending an authentication key to a mobile terminal in advance and passing the authentication key to an exchange from the mobile terminal when authentication is needed.

**SOLUTION:** A home memory 3 generates a temporary use key C which is characteristic of the mobile terminal 1. Then the temporary use key C and a mobile terminal number are both ciphered together with a secret key B. Further, the temporary use key C and the data ciphered with this secret key B are put together and the data ciphered with the secret key A are sent out to the mobile terminal 1. The mobile terminal 1 once receiving the ciphered data deciphers the data by using the secret key A to obtain the data ciphered with the temporary use key C and secret key B, and stored the data. When authentication is need, the mobile terminal 1 deciphers the data, ciphered with the secret key B, by using the secret key B to obtain the mobile terminal number and temporary use key C. Further, the mobile terminal number is confirmed and the mobile